

1 TRIAL & TECHNOLOGY LAW GROUP
2 A PROFESSIONAL CORPORATION
3 ROBERT A. SPANNER SBN 60308
3723 HAVEN AVENUE, SUITE 132
4 MENLO PARK, CA 94025
PHONE: (650) 324-2277
5 FAX: (650) 324-0178
email - ras@techtriallaw.com

6
7 Attorney for Plaintiffs

8 UNITED STATES DISTRICT COURT
9
10 NORTHERN DISTRICT OF CALIFORNIA
11 San Francisco Division

12
13 HENRY A. KLYCE and CAROLE M.
14 KLYCE,

15 Plaintiffs,

16 v.

17 DOES 1-10,

18 Defendants.
19 _____/

CASE NO. 11 CV 02248 WHA

**PLAINTIFFS' SUPPLEMENTAL *EX*
PARTE APPLICATION FOR LEAVE
TO TAKE FOLLOW-ON EXPEDITED
DISCOVERY, AND MOTION FOR
ORDER SHORTENING TIME**

20 As noted previously, this case involves an illegal Internet scheme, in which the identity
21 of the actual defendant is unknown and must be discovered. For a long period of time,
22 unidentified and unidentifiable persons had seized control of Plaintiff Carole Klyce' email
23 account, denying her access, deleting her saved email, and impersonating her by sending nasty
24 emails to her friends and family from her account.

25 On May 23, 2011 Plaintiffs brought an *ex parte* motion for expedited discovery
26

27
28 Mot. to Expedite Discovery
Case No. 11 CV 02248 WHA

1 pursuant to F.R.Civ.P. 26(f) in order to ascertain the identity of the defendant(s), and submitted
2 a proposed form of order regarding the procedure for propounding subpoenas (which the Court
3 signed the next day). Plaintiffs explained that discovery of the actual identity of the Defendants
4 was a three-step process: first, they first needed to subpoena from their own ISP's (Yahoo! and
5 AOL) the IP addresses of all persons who logged into Plaintiffs' email accounts and when the
6 log-ins occurred; second, Plaintiffs' expert could identify, by resort to an available Internet
7 directory, which ISP's were assigned those IP addresses at the particular times the illegal log-
8 ins occurred¹. Once the identification of the ISP for each illegal log-in is known, Plaintiffs can
9 then subpoena from those ISP's documents disclosing the actual identities of the persons
10 illicitly logging in to Plaintiffs' accounts (*see generally* original Declaration of Mark Seiden).
11 Once Yahoo! provided the IP addresses of the log-ins on June 29th, the identity of the ISP for
12 those IP addresses was constructively known, and the identities of the Doe Defendants can be
13 determined by subpoena. This supplemental *ex parte* motion seeks issuance of those
14 subpoenas².

15 After some wrangling, Yahoo produced responsive documents on June 29, 2011
16 without taking exception to any subpoena request, which was reasonably responsive given the
17 seventeen-day hold built into the Order to allow for third-party objections.
18
19
20
21

22
23 ¹ Contrary to common understanding, there is no one-to-one correspondence
24 between a particular IP address and a particular person (a static IP address); all ISP's now
use dynamic IP address assignment at the time of account log-in.

25 ² As was mentioned previously, ISP's believe they need court-ordered subpoenas in
26 light of the restrictions of the Cable Communications Policy Act, 47 U.S.C. §551(c)(2)
27 against disclosure of user information.

1 The documents produced by Yahoo! on June 28, 2011 identified hundreds of log-ins
2 into Plaintiff Carole Klyce' email account at Yahoo! by eight IP addresses (Spanner Decl., ¶2)
3 (plus a couple log-ins apiece by several other IP addresses which are being ignored for present
4 purposes). The documents were promptly turned over to Plaintiff's expert on June 29th
5 (Spanner Decl., ¶4), and Mr. Seiden identified the ISP's to whom these eight IP addresses
6 were assigned on June 30th: Comcast, Verizon, and Time Warner Cable (Seiden Decl., ¶3).

8 It was unfortunate that some of the Doe Defendants logging into Carole Klyce' account
9 came in through Comcast, because I discovered by perusal of Comcast's legal compliance
10 policies that Comcast retains log-in data for one of the shortest periods in the industry – only
11 six months (Spanner Decl., ¶3). Because some of the log-ins displayed in Yahoo's production
12 occurred in the first week of January, 2010 (Spanner Decl., ¶4), the information regarding the
13 identity of the persons logging in during early January will be lost; hence early issuance and
14 service of a subpoena is critical.³

16 In addition to Comcast, a large number of log-ins into Carole Klyce' account originated
17 from subscribers of two other ISP's – Time Warner Cable and Verizon (Seiden Decl., ¶ 3). By
18 this motion Plaintiff seeks Court approval for service of subpoenas upon Comcast, Time
19 Warner Cable, and Verizon for documents disclosing the identity of the approximately eight
20 persons who repeatedly logged into Carole Klyce' account⁴ without authorization or her
21

23 ³ A preservation demand was served on Comcast at its designated fax number for
24 receipt of subpoenas over the holiday weekend (Spanner Decl., ¶5).

25 ⁴ There were other ISP's from which other persons logged into Carole Klyce'
26 account, but the log-ins number only a handful; applying the rule of proportionality,
27 Plaintiff seeks to issue only the three subpoenas at this time. In addition, AOL has refused

1 knowledge. These eight persons are the Doe Defendants.

2 The standard for such expedited discovery is “good cause”. There is eminent good
3 cause for expedited discovery in this case for the purpose of identifying the Doe Defendants,
4 for without such discovery Plaintiffs obviously cannot proceed with their lawsuit because they
5 cannot serve the Complaint. In this Circuit,” where the identity of the alleged defendant[] [is]
6 not [] known prior to the filing of a complaint[,] the plaintiff should be given an opportunity
7 through discovery to identify the unknown defendants.” *Wakefield v. Thompson*, 177 F.3d
8 1160, 1163 (9th Cir. 1999), citing *Gillespie v. Civiletti*, 629 F.2d 637, 642 (9th Cir. 1980).
9

10 Cases such as this one – involving tortious or unlawful conduct committed over the
11 Internet – often require expedited discovery from the perpetrator’s ISP in order to discover the
12 perpetrator’s identity. Judges in this District apply the four-factor analysis set forth in
13 *Columbia Ins. Co. v. Seescandy.com*, 185 F.R.D. 573, 578-80 (N.D. Cal. 1999) to assess the
14 reasonableness of such a request⁵:
15

- 16 1) is there an identification of steps taken to locate the unidentified defendant;
- 17 2) has the absent defendant been described with sufficient specificity to be assured that
- 18 the defendant is a real person or entity susceptible to process in Federal court;
- 19 3) has the applicant set forth a justification for the specific discovery requested, and is
- 20 there a reasonable prospect that that discovery, from a limited number of persons or
- 21
- 22

23 _____
24 to respond to the subpoena served upon it until it received an administrative fee in advance
25 (already sent), so there is the possibility that a follow-on subpoena will be needed for Henry
Klyce’ account later.

26 ⁵ The order has been re-arranged for coherence.
27

1 entities, will lead to the identification of the absent defendant so that service can be
 2 effected;

3 4) are the claims against the absent defendant sufficient on their face.

4 Applying the four-factor test, “good cause” is apparent – especially in light of the fact that ISP’s
 5 retain log-in data for only limited periods.
 6

7 First, Plaintiffs have set forth what steps they have taken to identify the perpetrators of
 8 the misdeeds, and they have identified the miscreants with great specificity: only those persons
 9 who logged into Carole Klyce’ email account.
 10

11 Second (and third), an order for issuance of the subpoenas by the Court is certain to lead
 12 to the identification of the Defendant perpetrators and to the service of process upon them. The
 13 IP addresses of the perpetrators and the date and time of their log-in to Carol Klyce’ account
 14 have been disclosed; disclosure of their identity is identification of the Doe Defendants.

15 Fourth, the allegations of the Complaint clearly state claims for relief that would survive
 16 a motion to dismiss:
 17

18 **Stored Communications Act (First Cause of Action):** The Stored Communications
 19 Act, 18 U.S.C. §2701(a)(1) prohibits unauthorized access to an electronic communications
 20 service, and §2701(a)(2) prohibits anyone from obtaining, altering, or preventing authorized
 21 access to a wire or electronic communication while it is in electronic storage. Plaintiffs allege
 22 that their ISP was a stored communications service within the meaning of the statute, that the
 23 Doe Defendants accessed Yahoo! computers without authorization, that Plaintiffs’ account was
 24 unlawfully accessed and they themselves were denied access, and that their electronic
 25 communications were altered, all to their injury (Complaint, ¶¶7-14, 16-18).
 26
 27

1 **Computer Fraud and Abuse Act** (Second Cause of Action): The Computer Fraud and
 2 Abuse Act, 18 U.S.C. §1030(a)(5)(A) makes it unlawful to” knowingly cause[] the transmission
 3 of a program, information, code, or command, and as a result of such conduct, intentionally
 4 causes damage without authorization, to a protected computer”. Plaintiffs allege that the
 5 predator accessed Yahoo!’s computers without authorization, and thereupon loaded software or
 6 commands which enabled them to seize control of Plaintiffs’ email accounts, thus enabling them
 7 to block Plaintiffs’ access, destroy Plaintiffs’ files, and impersonate Plaintiff Carole Klyce by
 8 sending email from her account to her friends and family (Complaint, ¶¶8-10, 24-25).

9 **Comprehensive Computer Data Access and Fraud Act** (Third Cause of Action): This
 10 statute, Cal. Pen. Code §502(c)(1) *et. seq.*, states that anyone who “knowingly accesses and
 11 without permission alters, damages, deletes, destroys, or otherwise uses any data, computer,
 12 computer system, or computer network in order to . . . (A) devise or execute any scheme or
 13 artifice to defraud” is guilty of an offense. As noted above, Plaintiffs alleged that the intruder
 14 accessed Yahoo! computers and their account without authorization, and then altered and
 15 damaged their files. They also allege that the Doe defendant executed a scheme to defraud by
 16 impersonating Carole Klyce and sending emails from her account to her family and friends. In
 17 doing these acts, the Doe defendant also violated § 502(c)(2), which makes it unlawful to
 18 knowingly access and without permission take, copy or make use of any data from a computer;
 19 and §502(c)(4), which makes it unlawful to knowingly access and without permission to alter,
 20 damage, delete, or destroy any data on a computer. The absent defendant altered and damaged
 21 the data on Carole Klyce’ computer by deleting her email files, and altered Henry Klyce’s
 22
 23
 24
 25
 26
 27

1 account security information (Complaint, ¶¶29-34)⁶.

2 **E-Personation Statute (Fourth Cause of Action):** California just passed Pen. Code
3 §528.5, which prohibits impersonation of another person on the Internet. By sending emails
4 from Carole Klyce's account, the Doe defendant made her friends and family believe Carole
5 Klyce herself had sent them (Complaint, ¶¶41-42), thus violating the statute.
6

7 **Section 17200 Claim (Fifth Cause of Action):** The California unfair competition statute
8 was also violated (the "unlawful" prong) once any of the foregoing statutes were violated.
9

10 **Summary:** It is evident that the Plaintiffs have stated claims which would survive a
11 motion to dismiss.

12 In the Northern District of California good cause for expedited issuance of a subpoena to
13 an ISP to discover a miscreant's identity has invariably been found; *see, e.g., Solarbridge Tech.*
14 *v. John Doe*, 2010 U.S. Dist. LEXIS 97508, at *3-4 (N.D. Cal. Aug. 27, 2010); *IO Group, Inc.*
15 *v. Does 1 - 435*, 2011 U.S. Dist. LEXIS 14123, *2 (N.D. Cal. Feb. 3, 2011); *Zoosk Inc. v. Doe*,
16 2010 U.S. Dist. LEXIS 134292, *4-6 (N.D. Cal. 2010); *see also Liberty Media Holdings, LLC*
17 *v. Does 1-59*, 2011 U.S. Dist. LEXIS 7563, *3-8 (S.D. Cal. Jan. 25, 2011). Accordingly, an
18 order should issue authorizing service of subpoenas upon Comcast, Verizon, and Roadrunner in
19 accordance with the Court's order. A Proposed Order accompanies these motion papers.
20

21 **MOTION FOR ORDER SHORTENING TIME**

22 Because of the likelihood of destruction of log-in information (the incriminating
23 "fingerprint") by ISP's in the ordinary course of business (especially by Comcast), this Court is
24

25
26 ⁶ Indeed, Doe's conduct violated five independent provisions of the statute.

1 urged to rule on this motion as it did for the motion to issue subpoenas to Yahoo! and AOL, so
2 that the subpoenas may immediately issue.

3 Dated: July 7, 2011

Respectfully submitted,

4
5 TRIAL & TECHNOLOGY LAW GROUP
6 Attorneys for Plaintiffs
CAROLE AND HENRY KLYCE

7
8 /s/ Robert A. Spanner
By _____